ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

IN THE OF SOUTH CAROLINA COUNTY OF CHARLESTON	IN THE COURT OF COMMON PLEAS OF THE NINTH JUDICIAL CIRCUIT
JOE DOE, Plaintiff, v. TOWN OF MOUNT PLEASANT, OFFICER SHAWN FILLIAN, OFFICERS JANE and JOHN SMITH 1-6, Defendants.	Case No. 2022-CP-10- **COMPLAINT**

NOW COMES, the Plaintiff, Joe Doe, by and through undersigned counsel, brings this action against Town of Mount Pleasant (hereinafter TOMP), Officer Randall Fillian (hereinafter "Fillian"), and unknown Officer(s) Jane and John Smith 1-6 (hereinafter "Smith"), both individually and as agent(s) of the TOMP ("Defendants").

PRELIMINARY STATEMENT

1. Upon information, investigation and upon Plaintiff's own personal knowledge this action arises out of the June 19, 2020, wrongful intrusion into Plaintiff's private affairs and improper access to Plaintiff's personal information that was perpetrated against him by the Defendants, which held in its possession certain personal and protected health information (collectively, "the Private Information") of the Plaintiff.

2. The Private Information compromised in the violation of Plaintiff's personal and confidential information includes an incident report, photograph, personal names, treatment and clinical information, such as dates of evaluation, and information pertaining to Plaintiff's improper involuntary commitment and transport to Palmetto Behavioral Health.

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

3. The Breach was infiltrated by Defendants Fillian and Smith, Officers employed by TOMP who had no connection whatsoever to this incident other than to pry into matters they knew they were not supposed to be privy to for reasons which can only be presumed to be nefarious and with a purpose that they knew would do harm to Plaintiff.

4. Plaintiff Doe brings this case against Defendants for their failure to properly secure and safeguard the Private Information that Defendants acquired from its own actions from which Plaintiff could not defend against, and for the improper, intentional and unreasonable dissemination of such information to others.

5. Defendant TOMP acquired this information from Plaintiff as a result of forced interaction with Plaintiff, including without limitation, name and photo, among other things to be added based on discovery (collectively, "personal identifiable information" or "PII") as well as medical treatment/diagnosis information and medical record information (collectively "personal health information" or "PHI").

6. Defendant TOMP maintained the Private Information in a careless and reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to accessibility by uninterested officers and employees, essentially cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's Private Information was a known risk to Defendant TOMP, and thus TOMP was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in an unsecure and vulnerable condition.

7. In addition, TOMP and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had TOMP properly monitored its property and computer networks, it would have discovered and/or prevented the intrusion altogether.

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

8. Plaintiffs' personal and private information has now been disclosed to others, the full extent yet to be determined, and his privacy is now at risk as a result of Defendants' negligent and intentional conduct since the Private Information that TOMP collected and maintained has been disseminated.

9. Plaintiff's reputation has been besmirched and slandered, at least throughout the State of South Carolina, and the impact has resulted in embarrassment and humiliation as well as impacted his ability to be promoted in the workforce in the TOMP and afar.

10. By and through his Complaint, Plaintiff seeks to remedy these harms.

11. Plaintiff seeks remedies including, but not limited to, compensatory damages and punitive damages.

12. Accordingly, Plaintiffs bring this action against Defendants seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligent-hiring/training/supervision (iii) wrongful intrusion into private affairs/invasion of privacy, (iv) violation of South Carolina's data breach laws, S.C. Code § 39-1-90 (2009); (v) negligence *per se*; (vi) breach of fiduciary duty, and; (vii) breach of confidentiality.

PARTIES

13. Defendant TOMP is a municipal corporation organized under the laws of South Carolina with its principal place of business and services in Charleston County, South Carolina.

14. Defendant Ofc. Fillian, by information and belief, is a resident of Charleston County, South Carolina

15. Defendants, Officers Jane and John Smith 1-6 is a pseudonym for an unknown individual(s) whom are, by information and belief a resident of Charleston County, South Carolina.

16. Plaintiff Doe is a pseudonym for an individual and a resident of Charleston County State

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

of South Carolina. He received a notice from a TOMP police officer who received an email/text from Fillian with a copy of Plaintiff's private information, dated June 19, 2020, or on about that date. He is bringing this Action by way of pseudonym due to the sensitive and private nature of the allegations.

JURISDICTION AND VENUE

17. This Court has subject-matter jurisdiction over the claims in this lawsuit under South Carolina Code § 14-5-390.

18. This Court has personal jurisdiction over Defendants because it maintains its principal place of business and services in this county, regularly and systematically transacts business in this county with thousands of people from this county and its surrounding counties, and the wrong conduct complained of in this complaint occurred in this county.

19. Venue is proper in this county under South Carolina Code § 15-7-30 because Defendant has its principal place of business in this county and a substantial part of the events or omissions giving rise to this complaint occurred in this county.

BACKGROUND FACTS

20. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

21. TOMP is in the business of maintaining among other things, a Police Department.

22. In conjunction with maintaining a Police Department, TOMP has access and controls an extensive amount of Private Information (hereinafter PI). TOMP gather and create PI in its normal course of business/services from those with whom it interacts. TOMP retains this information on computer hardware – even after the interaction ends, some of it is subject to public dissemination and some of it private in nature and privileged from public dissemination.

23. Plaintiff was required to provide some of his most sensitive and confidential information,

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

including names, photograph, driver's license/ information, and health history.

24. Because of the highly sensitive and personal nature of the information TOMP acquires and stores with respect to its citizens, TOMP are required to maintain the privacy of certain information.

25. Upon information and belief, TOMP police officers were duped into responding to Plaintiff for an exaggerated complaint. The intrusive contact and incident was furthered worsened by the unconscionable scenario where Fillian and Smith, hacked Plaintiff's PI and disseminated it to slander Plaintiff.

26. Upon information and belief, the cyberattack was targeted at TOMP due to its status as a law enforcement/first responder/healthcare entity that collects, creates, and maintains both PII and PHI.

27. Upon information and belief, Fillian and Smith looked/hacked into the TOMP Police Computer/Network and exfiltrated personal information of Plaintiff after somehow learning that he was detained, questioned and committed for psychological evaluation. The targeted intrusion into the computer database attack was expressly designed to gain access to private and confidential data, including (among other things) the Private Information of Plaintiff's.

28. As a result of this targeted intrusion by Fillian and Smith and lack of supervision and security by TOMP, Fillian and Smith were able to copy the information and disseminate it at will to whomever they chose, sending said information across cellular/text/web. Had TOMP had the proper safety protocols in place, the attack would have been thwarted and not have occurred.

29. The Private Information contained in the TOMP computer/network was not encrypted nor filed into an available Confidential File Folder.

30. The exposed PI was compromised due to Defendants' negligent and/or careless acts and

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

omissions and failure to protect PI from TOMP's current and former employees.

31. By collecting and storing this personal information, TOMP had ethical duties to citizens and employees.

32. Plaintiff provided his PI to TOMP with the reasonable expectation and mutual understanding that TOMP would comply with its obligations to keep such information confidential and secure from unauthorized access.

TOMP Fails to Comply with Industry Standards

33. Experts studying cyber security routinely identify municipalities as being particularly vulnerable to cyberattacks because of the value of the PI which they collect and maintain.

34. Several best practices have been identified that a minimum should be implemented, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

35. Other best cybersecurity practices that are standard in the include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

36. TOMP failed to meet the minimum standards of any of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

TOMP's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

37. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive health information.

38. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

39. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data RSFH left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

40. TOMP's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

TOMP's Breaches

41. TOMP breached its obligations to Plaintiff and/or was otherwise negligent, careless and reckless because it failed to properly maintain and safeguard its computer systems and data, causing preventable harm. TOMP's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

b. Failing to adequately protect persons Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of emails containing PI;

e. Failing to ensure the confidentiality and integrity of electronic PI it created, received, maintained, and/or transmitted,

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of its workforces effectively on the policies and procedures regarding PI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PI, in violation of 45 C.F.R. § 164.530(b);

m. Failing to render the electronic PI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

n. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

PLAINTIFF's DAMAGES

42. To date, Defendants have done absolutely nothing to provide Plaintiff with relief for the damages he has suffered as a result of the Data Breach.

43. After the Data Breach, Plaintiff experienced actual denial of a promotion based on knowledge of this event. Plaintiff also has received a number of notifications about notice of his commitment.

44. Plaintiff suffered actual injury in the form of embarrassment and humiliation. He fears that he is judged and looked at differently. Although ultimately the commitment was deemed not necessary, improper, against proper protocol and procedure and unlawfully what the public knows is that he was involuntarily committed.

45. Plaintiffs' PI was compromised as a direct and proximate result of Defendants' actions, or failures to act.

46. As a direct and proximate result of Defendants' conduct, Plaintiff has been placed at an imminent, immediate, and continuing increased risk of reputation, employment and embarrassment.

47. As a direct and proximate result of Defendant's conduct, Plaintiff has been forced to expend time dealing the intrusive cyberattack, breach, and attack to his PI.

48. Further, as a result of Defendants' conduct, Plaintiff is forced to live with the anxiety that his Private Information—which contains the most intimate details about a person's life, may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving him of any right to privacy whatsoever.

49. As a direct and proximate result of Defendants' actions and inactions, Plaintiff has suffered a loss of privacy and are at an imminent and increased risk of future harm.

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

FOR A FIRST CAUSE OF ACTION
(Negligence)

50. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein

51. As a condition of interaction with Defendants, Defendants' current and former citizens/employees (including Plaintiff) are/were obligated to provide Defendants with certain non-public PII and PHI, including their names, addresses, dates of birth, Social Security numbers, driver's license/state ID numbers, passport numbers, credit/debit card information, financial account information, health insurance information.

52. As a condition of their interaction with Defendants, Defendants created PII and PHI for citizens/employees, current and former (including Plaintiff), including, medical treatment/diagnosis information, medical record information, and health/mental health claims information.

53. Plaintiff entrusted his PII and PHI to Defendants on the premise and with the understanding that Defendants would safeguard his information, use his PII and PHI for official purposes only and/or not to disclose their PII and PHI to unauthorized/authorized third parties.

54. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing and using of its current and former citizens/employees PII and PHI involved an unreasonable risk of harm to Plaintiff, even if the harm occurred through the criminal acts of a third party.

55. Defendants had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing Defendants'

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

security protocols to ensure that Plaintiff's information in Defendants' possession was adequately secured and protected.

56. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former PII it was no longer required to retain pursuant to regulations.

57. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse or Plaintiff's PII and PHI.

58. By collecting and storing this data in its computer/network property, Defendants had a duty of care to use reasonable means to secure and safeguard its computer/network property and Plaintiff's Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach and/or Data Breach.

59. Defendants owed a duty of care to the Plaintiff to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

60. Defendants' duty to use reasonable security measures under HIPAA, required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

61. In addition, Defendant TOMP had a duty to employ reasonable security measures under

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

62. Defendants duty to use reasonable security measures arose as result of the special relationship that existed between Defendant and Plaintiff. That special relationship arose because Plaintiff entrusted Defendants with his confidential PII and PHI, a necessary and required, voluntary or involuntary, part of obtaining services from Defendants.

63. Defendants were subject to an "independent duty," untethered to any agreement between Defendant and Plaintiff.

64. A breach of security, unauthorized access and resulting injury to Plaintiff was reasonably foreseeable, particularly in light of TOMP's inadequate security practices.

65. Plaintiff was a foreseeable victim of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff, the critical importance of providing adequate minimum security of that PII and PHI, and the necessity for encrypting PII and PHI stored on TOMP's systems.

66. Defendants own conduct created a foreseeable risk of harm to Plaintiff. Defendants' misconduct included but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included its decision not to comply with industry standards for safekeeping of Plaintiff's PII.

67. Plaintiff had no ability to protect his PII and PHI that was in, and possibly remains in, Defendants' possession.

68. Defendants were in a position to protect against the harm suffered by Plaintiff as a result of the Data Breach.

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

69. Defendants had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiff within Defendants possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff to take steps to prevent, mitigate and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

70. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of Plaintiff's PII and/or PHI.

71. Defendants have admitted that Plaintiff's PII and PHI was wrongfully lost, misplaced and/or disclosed to unauthorized/authorized third persons as a result of the Data Breach.

72. Defendants have admitted that the breach was preventable by enhancing security, training and providing continued education to staff on PII and PHI protection.

73. Defendants, through its actions and/or omissions, unlawfully breached its duties to Plaintiff by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's PII and PHI during the time the PII and PHI was within Defendants' possession or control.

74. Defendants improperly and inadequately safeguarded the Plaintiff's PII and PHI in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

75. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former citizens/employees PII and PHI in the face of increased risk of theft.

76. Defendants through its actions and/or omissions unlawfully breached its duty to Plaintiff by failing to have appropriate procedures in place to detect and prevent dissemination of PII and PHI.

77. Defendants breached its duty to exercise appropriate clearinghouse practices by failing to

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

remove PII and PHI it was no longer required to retain pursuant to regulations.

78. Defendants, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff the existence and scope of the Data Breach.

79. But for the Defendants' wrongful and negligent breach of duties owed to Plaintiff, the Plaintiff's PII and PHI would not have been compromised.

80. There is a close causal connection between TOMP's failure to implement security measures to protect Plaintiff's PII and PHI and the harm suffered or risk of imminent harm suffered by Plaintiff. Plaintiff's PII and PHI was misplaced, accessed, and disseminated as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing and maintaining appropriate security measures.

81. As a direct and proximate result of Defendants' negligence, Plaintiff has suffered and will suffer injury including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how his PII and PHI is used; (iii) the compromise, publication and/or theft of the PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud and/or unauthorized use of their PII and PHI: (v) lost opportunity costs associated with effort expanded and the lost productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI which remain in Defendants' possession is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI in its continued possession; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PII and PHI

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

compromised as a result of the Data Breach for the remainder of the lives of the Plaintiff.

82. As a direct and proximate result of Defendants' negligence, Plaintiff has suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy and other economic and non- economic losses.

83. As a direct and proximate result of Defendants' negligence, Plaintiff has suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI in their continued possession.

84. As a direct and proximate result of Defendants' negligence, Plaintiff are entitled to punitive damages to be determined by the trier of fact due to the Defendants' reckless indifference to safeguard his information, as shown by the repeated instances of data breaches that have incurred known and unknown.

FOR A SECOND CAUSE OF ACTION
(Negligent Hiring/Training/Supervision) As To Defendant TOMP

85. The Plaintiff re-alleges and incorporates by reference all allegations set forth above as if repeated verbatim.

86. TOMP individually or by and through their employees, agents, and legal representatives owed Plaintiff, as a member of the general public and employee duties of care.

87. TOMP individually or by and through their employees, agents, and/or legal representatives owed Plaintiff, as a member of the general public/employee, duties of care not to allow other employees/agents to commit an cyberattack/assault on Plaintiff's PII and/or PHI and to protect Plaintiff, as a member of the general public/employee, from the consequences of its employees/agents actions, to which the TOMP contributed.

88. TOMP by and through their employees, agents, and legal representatives breached this duty

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

by allowing Defendants Fillian and Smith to disseminate Plaintiff's PII and PHI and by not protecting Plaintiff.

89. TOMP individually and/or by and through their employees, agents, and/or legal representatives breached its duty to protect Plaintiff further by:

1. Hiring employees with no formal training on PII and PHI;
2. Hiring employees who are not equipped or trained to handle PII and PHI;
3. Failing to perform reasonable training on PII and PHI security;
4. Failing to properly secure the police Computer/Network by monitoring incidents involving confidential information;
5. Negligent hiring of employees, law enforcement officers;
6. Negligent training of employees, law enforcement officers;
7. Negligent supervision of employees, law enforcement officers;
8. Negligently allowing and/or encouraging employees, law enforcement officers; to engage in gossip, libel, slander;
9. Failing to maintain proper control of employees, law enforcement officers;
10. Other particulars that will be discovered prior to trial.

90. The violent attack on Plaintiff's PII and PHI were a direct and proximate result of the breach of duty by the TOMP, individually and/or by and through their employees, agents, and representatives.

91. As a direct and proximate result of the TOMP, individually and/or by and through its employees, agents, and legal representatives, willful, wanton, reckless, grossly negligent, and negligent acts as set forth above, Plaintiff suffered the following damages:

1. Physical pain and suffering;

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

2. Mental anguish;
3. Shock and injury to Plaintiff;
4. Bills and other economic loss;
5. Impairment of health and bodily efficiency;
6. Loss of Plaintiff's enjoyment of life;
7. Embarrassment;
8. Permanent social injuries;
9. Increased susceptibility to future injury;
10. Future expenses; and
11. Other damages which will be shown at trial.

FOR A THIRD CAUSE OF ACTION
(Wrongful Intrusion Into Private Affairs/Invasion of Privacy)

92. Plaintiffs incorporate by reference all preceding allegations as though fully set forth herein.

93. Plaintiff had a legitimate expectation of privacy to his PII and PHI and was entitled to the protection of this information against disclosure to unauthorized third parties.

94. Defendants owed a duty to Plaintiff to keep his PII and PHI confidential.

95. Defendants failed to protect and released to unknown and unauthorized third parties the Plaintiff's PII and/or PHI.

96. Defendants allowed unauthorized and unknown third parties access to and examination of Plaintiff's PII and/or PHI by way of Defendants' failure to protect the PII and PHI.

97. The unauthorized release to, custody of, and examination by unauthorized third parties of the Plaintiff's PII and/or PHI is highly offensive to a reasonable person.

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

98. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff disclosed his PII and PHI to TOMP, or allowed TOMP to create their PII and PHI, as part of the involuntary and intrusive interaction by Defendant, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff was reasonable in his belief that such information would be kept private and would not be disclosed without his authorization.

99. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiff's interest in solitude or seclusion, either as to his person or as to their private affairs or concerns that would be highly offensive to a reasonable person.

100. Defendants acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

101. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff.

102. As a proximate result of the above acts and omissions of Defendants, the PII and PHI of Plaintiff was disclosed to third parties without authorization, causing Plaintiff to suffer damages.

103. Unless and until enjoined and restrained by Order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff in that the PII and PHI maintained by Defendant can be viewed, distributed and used by unauthorized persons for years to come. The Plaintiff shall have no adequate remedy at law for the injuries in that judgment for monetary damages will not end the invasion of privacy for Plaintiff.

FOR A FOURTH CAUSE OF ACTION

(Violation of South Carolina's Data Breach Laws S.C. CODE § 39-1-90) As To Defendant TOMP

104. Plaintiffs incorporate by reference, all preceding allegations as though fully set forth

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

herein.

105. In pertinent part, S.C. Code § 39-1-90 provides:

"A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption , redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. The disclosures must be made in the most expedient time possible and without unreasonable delay…"

106. TOMP owns, licenses and/or maintains computerized data that includes Plaintiff's PII and PHI.

107. TOMP's conduct, as alleged above, violated the data breach statute of South Carolina, S.C. Code § 39-1-90.

108. TOMP was required, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyber security incident described herein.

109. The Data Breach constituted a "breach of the security system" within the meaning of § 39-1-90.

110. The information compromised in the Data Breach constituted "personal identifying information" within the meaning of § 39-1-90.

111. TOMP admits that the illegal use of the information had occurred or was reasonably likely to occur or that the use of the information created a material risk of harm to Plaintiff.

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

112. TOMP violated § 39-1-90 by unreasonably delaying disclosure of the Data Breach to Plaintiff, whose personal identifying information was, or reasonably believed to have been, acquired by an unauthorized person.

113. As a result of TOMP's violation of S.C. Code § 39-1-90, Plaintiff incurred damages as alleged herein.

114. Plaintiff seeks all remedies available under S.C. Code § 39-1-90, including, but not limited to: (a) actual damages suffered as alleged above; (b) statutory damages for TOMP's willful, intentional, and/or reckless conduct; (c) equitable relief; and (d) reasonable attorneys' fees and costs.

FOR A FIFTH CAUSE OF ACTION
(Negligence *Per Se*)

115. Plaintiffs incorporate by reference, all preceding allegations as though fully set forth herein.

116. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision- making.

117. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

118. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

119. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"). Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

120. These FTC enforcement actions include actions against healthcare and healthcare like providers like Defendant.

121. TOMP failed to properly implement basic data security practices, including (upon information and belief) failing to implement multifactor authentication. TOMP's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

122. TOMP was at all times fully aware of its obligation to protect PII and PHI. TOMP was also aware of the significant repercussions that would result from its failure to do so.

123. Pursuant to Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), TOMP had a duty to provide fair and adequate computer systems and data security practices to safeguard

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

Plaintiff's Private Information.

124. An essential purpose of Section 5 of the FTCA is to protect against the kind of harm that Plaintiff suffered here – unauthorized access to PII and PHI.

125. Plaintiff is within the class of persons that the FTCA was intended to protect.

126. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff.

127. TOMP's failure to comply with applicable laws and regulations constitutes negligence per se.

128. But for TOMP's wrongful and negligent breach of its duties owed to Plaintiff, Plaintiff would not have been injured.

129. The injury and harm suffered by Plaintiff was the reasonably foreseeable result of TOMP's breach of its duties. TOMP knew or should have known that it was failing to meet its duties, and that TOMP's breach would cause Plaintiff to experience the foreseeable harms associated with the exposure of their Private Information.

130. As a direct and proximate result of TOMP's negligent conduct, Plaintiff has suffered injury and is entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOR AN SIXTH CAUSE OF ACTION
(Breach of Fiduciary Duty)

131. Plaintiffs incorporate by reference, all preceding allegations as though fully set forth herein.

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

132. In light of the special relationship between Defendant and Plaintiff, whereby Defendants became entrusted with, and the guardian of Plaintiff's Private Information, Defendants became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of those it services, including Plaintiff, (1) for the safeguarding of Plaintiff's Private Information; (2) to timely notify Plaintiff of a Data Breach and/or data breach and disclosure; and (3) maintain complete and accurate records of what information (and where) Defendant did and does store.

133. Defendants have a fiduciary duty to act for the benefit of Plaintiff upon matters within the scope of its relationship, in particular, to keep secure the Private Information.

134. Defendants breached its fiduciary duties to Plaintiff by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

135. Defendants breached its fiduciary duties to Plaintiff by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's Private Information.

136. Defendants breached its fiduciary duties owed to Plaintiff by failing to timely notify and/or warn Plaintiff of the Data Breach.

137. Defendants breached its fiduciary duties owed to Plaintiff by failing to ensure the confidentiality and integrity of electronic PHI TOMP created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

138. Defendants breached its fiduciary duties owed to Plaintiff by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

139. Defendants breached its fiduciary duties owed to Plaintiff by failing to implement policies

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

140. Defendants breached its fiduciary duties owed to Plaintiff by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

141. Defendants breached its fiduciary duties owed to Plaintiff by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

142. Defendants breached its fiduciary duties owed to Plaintiff by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

143. Defendant breached its fiduciary duties owed to Plaintiff by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

144. Defendants breached its fiduciary duties owed to Plaintiff by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

145. Defendants breached its fiduciary duties owed to Plaintiff by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. §

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

164.308(a)(5).

146. Defendants breached its fiduciary duties owed to Plaintiff by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

147. Defendants breached its fiduciary duties to Plaintiff by otherwise failing to safeguard Plaintiff's Private Information.

148. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff has suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the life of Plaintiff.

149. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff has suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

FOR A SEVENTH CAUSE OF ACTION
(Breach of Confidentiality)

150. Plaintiffs adopt by reference all allegations contained in the paragraphs above as if fully set forth herein.

151. At all relevant times, Defendants owed a duty to Plaintiff to maintain the confidentiality of his medical records, documentation and information against unauthorized and/or unconsented disclosure and to maintain the safety, security and privacy of their patient's medical, personal and financial information.

152. At all relevant times, Defendants owed a special and continuing duty of care to Plaintiff to maintain the safety, security and privacy of his medical and personal health information. Evidence of this duty was the Defendants notification/investigation that the information they were entrusted with had been compromised. This duty requires Defendants to maintain the privacy of personal information, and that Plaintiff is required to be notified, if his information is acquired, used, or shared in a manner not permitted under law.

153. Defendants breached their duties to the Plaintiff by allowing the disclosure, dissemination and distribution of his PII and PHI records without Plaintiff's permission or consent.

154. As a direct, proximate, immediate, and foreseeable result of the acts and omissions of Defendants, the Plaintiff has suffered damages, economic, non-economic, and mental anguish as a result of the aforementioned data breach, including but not limited to expenses and costs of credit monitoring, lost time, fraud protection, identity theft, as well as the increased and actual harm of identity theft- all of which would never have been suffered but for the negligent acts and omissions of Defendants. Because the acts and omissions of Defendants have been repeated and continue to occur, Defendant should be punished by punitive damages as determined by the trier of fact.

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

FOR AN EIGHTH CAUSE OF ACTION
(Violation of the Computer Fraud and Abuse Act)

155. Plaintiff adopts by reference all allegations contained in the paragraphs above as if fully set forth herein.

156. Defendant, TOMP's computer fits within the definition of 'computer' per the Computer Fraud and Abuse Act ("CFAA), 18 USC §1030 (e)(1), and by being connected to the Internet and being used regularly in interstate commerce and communications is a "protected computer" as understood in the CFAA. §1030(e)(1).

157. Defendants authorized and made accessible Plaintiff's data without authorization in violation of the CFAA.

158. The access of the records exceeded authorization and was for no proper purpose.

FOR AN NINTH CAUSE OF ACTION
(Violation of the SC Computer Crime Act)

159. Plaintiff adopts by reference all allegations contained in the paragraphs above as if fully set forth herein.

160. Defendant, TOMP'S computer fits within the definition of SC Code of Laws §16-16-10 definition of computer and actions conducted by Defendants are in violation of this section.

161. The access of the records exceeded authorization and was for no proper purpose.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment in their favor and against Defendants as follows:

A. For equitable relief enjoining Defendants from engaging in the wrong conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's PII and PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff;

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

B. For an award of damages, including actual, compensatory, nominal, consequential damages, and punitive damages as allowed by law in an amount to be determined;

C. Scheduling a trial by jury in this action;

F. Awarding Plaintiffs' reasonable attorneys' fees, costs and expenses, as permitted by law;

G. Awarding pre and post-judgment interest on any amounts awarded, as permitted by law; and

H. Awarding such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand that this case be tried by a jury on all counts.

Respectfully submitted this 13th of JUNE, 2022.

SLOTCHIVER & SLOTCHIVER, LLC

s/Daniel Scott Slotchiver
Daniel Scott Slotchiver (SC Bar No. 15129)
Slotchiver & Slotchiver LLP
751 Johnnie Dodds Blvd, Suite 100
Mt. Pleasant, South Carolina 29464
Phone: 843-577-6531
dan@slotchiverlaw.com

-AND-

s/Edward L Phipps
Edward L. Phipps (SC Bar No. 70252)
Phipps Law Firm, LLC
571 Savannah Highway
Charleston, SC 29407
Phone: 843-300-4444
edward@phippslawfirm.com

Attorneys for Plaintiff

ELECTRONICALLY FILED - 2022 Jun 13 2:06 PM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

IN THE OF SOUTH CAROLINA COUNTY OF CHARLESTON	IN THE COURT OF COMMON PLEAS OF THE NINTH JUDICIAL CIRCUIT
JOE DOE, Plaintiff, v. TOWN OF MOUNT PLEASANT, OFFICER SHAWN FILLIAN, OFFICERS JANE and JOHN SMITH 1-6, Defendants.	Case No. 2022-CP-10- **SUMMONS**

TO THE ABOVE-NAMED DEFENDANTS:

YOU ARE HEREBY SUMMONED and required to answer the Complaint in this action, a copy of which is hereby served upon you herewith, and to serve a copy of your Answer to said Complaint on the subscribers at their offices, Slotchiver & Slotchiver, LLC, 751 Johnnie Dodds Blvd., Suite 100, Mt. Pleasant, South Carolina 29464 or The Phipps Law Firm, LLC, 571 Savannah Highway, Charleston, South Carolina 29407 or to otherwise appear and defend, within thirty (30) days after the service hereof, exclusive of the day of such service. If you fail to answer the Complaint, or otherwise to appear and defend, within the time aforesaid, the Plaintiff in this action will apply to the Court for judgment by default to be rendered against you for the relief demanded in the Complaint.

By: *s/Daniel Scott Slotchiver*

Daniel Scott Slotchiver (SC Bar No. 15129)
751 Johnnie Dodds Blvd, Suite 100
Mt. Pleasant, South Carolina 29464
Phone: 843-577-6531
dan@slotchiverlaw.com

-AND-

s/Edward L Phipps
Edward L. Phipps (SC Bar No. 70252)
571 Savannah Highway
Charleston, SC 29407
Phone: 843-300-4444
edward@phippslawfirm.com
Attorneys for Plaintiff

June 13, 2022
Charleston, SC

ELECTRONICALLY FILED - 2022 Jul 12 11:23 AM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

STATE OF SOUTH CAROLINA COUNTY OF CHARLESTON Joe Doe, Plaintiff, vs. Town of Mount Pleasant, Officer Shawn Fillian, Officers Jane and John Smith 1-6, Defendants.	IN THE COURT OF COMMON PLEAS FOR THE NINTH JUDICIAL CIRCUIT CASE NO.: 2022-CP-10-2665 **ACCEPTANCE OF SERVICE**

I, David G. Pagliarini, Esq., hereby accept and acknowledge receipt and service upon me, as attorney for the Town of Mount Pleasant, South Carolina, a filed copy of the Summons and Complaint on behalf of Defendant the Town of Mount Pleasant, South Carolina June 22, 2022.

/s/ David G. Pagliarini
David G. Pagliarini, S.C. Bar No. 8850
Corporation Counsel
Town of Mount Pleasant
100 Ann Edwards Lane
Mount Pleasant, SC 29464
(843) 884-8517
Dpagliarini@tompsc.com

ELECTRONICALLY FILED - 2022 Jul 12 11:23 AM - CHARLESTON - COMMON PLEAS - CASE#2022CP1002665

STATE OF SOUTH CAROLINA
COUNTY OF CHARLESTON

IN THE COURT OF COMMON PLEAS
CASE NUMBER: 2022CP1002665

Joe Doe

Plaintiff(s),

v.

Town of Mount Pleasant, Officer Shawn Fillian, Officers Jane and John Smith 1-6,

Defendant(s)

AFFIDAVIT OF SERVICE

ORIGINAL

The undersigned, Delano Francis, being first duly sworn; states that on the 27th day of June, 2022 at 12:49 a.m./p.m. served:

- [X] Summons and Complaint
- [ ] Answer
- [ ] Answer and Counterclaim
- [ ] Request to Admit
- [ ] Request to Produce
- [ ] Interrogatories
- [ ] Motion
- [ ] Order
- [ ] Subpoena
- [ ] Decree
- [ ] Subpoena Duces Tecum
- [ ] Order for Continuance
- [ ] Other

In the within action by delivering a certified copy thereof to:

- [ ] Plaintiff personally
- [X] Other (name) Defendant, Officer Shawn Fillian
  - [ ] A person of discretion who resides at the residence of the person named for service and for that person
  - [ ] A person of discretion at the business of the person named for service

Height_____ Weight_____ Hair Color_____ Eyes_____ Age_____
Clothing MT. Pleasant Police Department Uniform

At: MT. Pleasant Police Department 100 Ann Edwards In. MT Pleasant SC 29464

Summary of Service:

Sworn to and subscribed before me
On this 27 day of June, 2017

Notary Public for South Carolina
County of Charleston
My commission expires: 11/18/2031

Signature of Process Server

JOCELYN B. LATIMER
Notary Public - State of South Carolina
My Commission Expires
11/18/2031